

IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD*

Fresly Nandar Pabokory¹⁾, Indah Fitri Astuti²⁾, Awang Harsa Kridalaksana³⁾

^{1,2,3)}Program Studi Ilmu Komputer, FMIPA, Universitas Mulawarman
Email : fres_comsc@yahoo.com¹⁾, indahfitriastuti@yahoo.com²⁾, awangkid@gmail.com³⁾

ABSTRAK

Perkembangan teknologi terutama pada sistem pengamanan data dalam menjaga keamanan data informasi telah berkembang pesat. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi dan steganografi. Pada penerapannya dilakukan tidak hanya pada satu teknik keamanan saja, melainkan bisa dilakukan dengan kombinasi dalam keamanan data informasi. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada pesan teks, isi *file* dokumen, dan *file* dokumen dengan melakukan perhitungan algoritma *Advanced Encryption Standard* (AES). AES merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data dimana algoritmanya adalah *blockchiptext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Hasil dari penelitian yaitu pengguna dapat mengenkripsi pesan teks kemudian disimpan menjadi sebuah *file* dokumen dan isi *file* dokumen tersebut dienkripsi lagi selanjutnya hasil enkripsi isi *file* dokumen tersebut, *file* dokumennya dienkripsikan dan selanjutnya dikompresi dan disembunyikan pada sebuah *file* citra (gambar) agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian yang berlapis-lapis.

Kata kunci : Kriptografi, *Advanced Encryption Standard* (AES), Pesan Teks, Isi *File* Dokumen, Steganografi

PENDAHULUAN

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Dari hal penggunaan komputerisasi tersebut, maka dibuatlah sebuah keamanan bagi seluruh aset-asetnya, terutama informasi-informasi dan data-data penting demi menjaga kerahasiaan informasi data tersebut. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman yang mungkin timbul. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi.

Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi dan teknik penyembunyian data yang disebut dengan steganografi.

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa.

Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut.

Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai *chiphertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut enkripsi (*encryption*), dan proses pengembalian dari *ciphertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*).

Dalam hal ini *file* yang dapat di enkripsi adalah *file* dokumen berupa teks, *file* citra berupa gambar, serta *file* audio dan *file* video dalam format digital. Pada pesan teks, isi *file* dokumen, atau *file* dokumen dalam menjaga kerahasiaan informasi datanya memerlukan teknik-teknik enkripsi dan dekripsi yang tidak mudah atau sukar untuk dipecahkan. Proses pengamanan pada pesan teks, isi *file* dokumen, atau *file* dokumen dapat dilakukan dengan mengenkripsi pesan teks, isi *file* dokumen, atau *file*

dokumen tersebut dengan menggunakan metode algoritma tertentu yang dapat membuat data informasi tersebut tidak bisa dibaca atau tidak dapat dimengerti oleh pihak lain. Salah satunya dengan menggunakan metode algoritma *Advanced Encryption Standard* (AES). Algoritma *Advanced Encryption Standard* (AES) dipilih penulis dalam menjaga keamanan pada sebuah data atau informasi tersebut, dikarenakan AES merupakan *cipher* yang berorientasi pada bit, sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam *software* dan *hardware*. AES memiliki ketahanan terhadap semua jenis serangan yang diketahui. Disamping itu kesederhanaan rancangan, kekompakan kode yang sederhana dan kecepatan pada berbagai platform dimiliki oleh algoritma AES. AES terbukti kebal menghadapi serangan konvensional (*linear* dan *diferensial attack*) yang menggunakan statistik untuk memecahkan sandi, dan dalam setiap proses enkripsi dan dekripsi harus melakukan 10 perputaran atau 10 iterasi (10 *Round*) dalam melakukan pengamanan maupun untuk membuka pengamanan tersebut.

Dalam hal ini juga ditambahkan sebuah sistem pendukung pada pengamanan data setelah melakukan teknik kriptografi dalam menjaga keamanan data informasi tersebut yaitu dengan teknik penyembunyian data atau disebut steganografi. Steganografi merupakan seni dan ilmu untuk menyembunyikan pesan dalam sebuah media pesan. Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama dalam steganografi. Dengan metode steganografi, pesan yang ingin disampaikan disembunyikan dalam suatu media umum sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak diinginkan untuk mengetahui pesan rahasia tersebut. Salah satu implementasi *steganography modern* adalah pada media citra digital.

Dalam metode steganografi untuk menyembunyikan suatu pesan ke dalam *file* digital (*file* citra, *file* audio, dan *file* video). Sebagai contoh yaitu media citra digital sebagai pesan yang akan dikirim terlebih dahulu disisipkan atau disembunyikannya suatu pesan rahasia ke dalam *file* citra tersebut. Pada *file* citra yang telah disisipkan suatu pesan tersebut tidak akan terlihat jelas atau diketahui oleh pihak lain bahwa *file* citra tersebut terdapat suatu pesan rahasia didalamnya kecuali pengirim dan penerima yang mengetahui bahwa ada pesan rahasia.

Dalam hal ini penulis menggunakan sistem keamanan pendukung steganografi dengan teknik *simple* yaitu menyembunyikan sebuah pesan atau *file* rahasia yang telah terenkripsi ke dalam *file* citra (gambar) menggunakan *command/DOS*. Hal ini bertujuan agar pesan atau *file* rahasia tersebut tidak dapat diketahui oleh pihak lain.

Berdasarkan uraian di atas, dilakukan penelitian yang lebih mendalam mengenai metode kriptografi *Advanced Encryption Standard* (AES) dan steganografi dengan mengambil konsep judul

yaitu "Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi *File* Dokumen, dan *File* Dokumen Menggunakan Algoritma *Advanced Encryption Standard*".

TINJAUAN PUSTAKA

Dokumen Digital

Dokumen merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain. Dokumen meliputi berbagai kegiatan yang diawali dengan bagaimana suatu dokumen dibuat, dikendalikan, diproduksi, disimpan, didistribusikan, dan digandakan. Dokumen digital merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya [4].

Citra

Citra adalah gambar dua dimensi yang dihasilkan dari gambar analog dua dimensi yang *continue* menjadi gambar diskrit melalui proses *sampling*. Setiap elemen pada citra dibentuk dari *pixel-pixel*. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu *Red*, *Green*, *Blue*.

Kompresi File (*File Compress*)

Kompresi *file* adalah suatu cara untuk mengkodekan informasi dengan menggunakan *bit* yang lebih rendah yang digunakan untuk memperkecil ukuran data agar dapat disimpan dengan ruang penyimpanan yang kecil dan juga dapat mempersingkat waktu dalam transfer data.

File

File adalah entitas dari data yang disimpan didalam sistem *file* yang dapat diakses dan diatur oleh pengguna. Sebuah *file* memiliki nama yang unik dalam direktori di mana ia berada. Alamat direktori dimana suatu berkas ditempatkan diistilahkan dengan *path*.

Sebuah *file* berisi aliran data (atau data stream) yang berisi sekumpulan data yang saling berkaitan serta atribut berkas yang disebut dengan properties yang berisi informasi mengenai *file* yang bersangkutan seperti informasi mengenai kapan sebuah berkas dibuat.

METODE KEAMANAN DATA

Ada 2 metode keamanan data yang digunakan yaitu Kriptografi menggunakan algoritma *Advanced Encryption Standard* (AES) dan Steganografi menggunakan *Command/DOS*.

Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi).

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau *terminology*. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, *Plainteks*, dan *Cipherteks*

Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*).

2. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan.

3. Enkripsi dan dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan cipherteks menjadi plainteks semula disebut dekripsi (*decryption*) atau *deciphering* (standard nama menurut ISO 7498-2).

4. *Cipher* dan kunci

Algoritma kriptografi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan cipherteks, maka :

$$E(P) = C \rightarrow \text{fungsi enkripsi } E \text{ memetakan } P \text{ ke } C$$

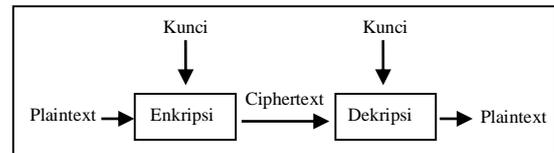
$$D(C) = P \rightarrow \text{fungsi dekripsi } D \text{ memetakan } C \text{ ke } P$$

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan $D(E(P)) = P$ harus benar.

Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini

algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa *string* atau deretan bilangan.

Dengan menggunakan kunci K , maka fungsi enkripsi dan dekripsi dapat ditulis sebagai skema diperlihatkan pada Gambar 1.



Gambar 1. Skema enkripsi dan dekripsi dengan menggunakan kunci

Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan *cipher* substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain.

Tujuan kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. Kerahasiaan (*confidentiality*)

Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. Integritas data (*data integrity*)

Adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.

3. Otentikasi (*authentication*)

Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*).

4. *Non-repudiation*

Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

Advanced Encryption Standard (AES)

Pada tahun 1997 kontes pemilihan suatu standar algoritma kriptografi baru pengganti DES dimulai dan diikuti oleh 21 peserta dari seluruh dunia.

Setelah melewati tahap seleksi yang ketat, pada tahun 1999 hanya tinggal 5 calon yaitu algoritma *Serpent* (Ross Anderson-*University of Cambridge*, Eli Biham-*Technion*, Lars Knudsen-*University of California San Diego*), *MARS* (IBM Amerika), *Twofish* (Bruce Schneier, John Kelsey, dan Niels Ferguson-*Counterpane Internet Security Inc*, Doug

Whiting-Hi/fn Inc, David Wagner-University of California Berkeley, Chris Hall-Princeton University), Rijndael (Dr. Vincent Rijmen-Katholieke Universiteit Leuven dan Dr. Joan Daemen-Proton World International), dan RC6 (RSA Amerika).

Setahun kemudian pada tahun 2000, algoritma Rijndael terpilih sebagai algoritma kriptografi yang selain aman juga efisien dalam implementasinya dan dinobatkan sebagai AES. Nama Rijndael sendiri berasal dari gabungan nama penemunya.

Deskripsi Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blokchipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Perbandingan jumlah proses yang harus dilalui untuk masing-masing masukan diperlihatkan pada tabel 1.

Tabel 1. Jumlah proses berdasarkan bit blok dan kunci

Panjang Kunci Dalam bit	Panjang Kunci (Nk) Dalam words	Ukuran Blok Data (Nb) Dalam words	Jumlah Proses (Nr)
128	4	4	10
192	6	4	12
256	8	4	14

Blok-blok data masukan dan kunci dioperasikan dalam bentuk array. Setiap anggota array sebelum menghasilkan keluaran ciphertext dinamakan dengan state. Setiap state akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, AddRoundKey, SubBytes, ShiftRows, dan MixColumns. Kecuali tahap MixColumns, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap MixColumns tidak akan dilakukan pada tahap terakhir. Proses dekripsi adalah kebalikkan dari dekripsi.

Karena terjadi beberapa tahap dalam proses enkripsi, maka diperlukan subkey-subkey yang akan dipakai pada tiap tahap. Pengembangan jumlah kunci yang akan dipakai diperlukan karena kebutuhan subkey-subkey yang akan dipakai dapat mencapai ribuan bit, sedangkan kunci yang disediakan secara default hanya 128-256 bit. Jumlah total kunci yang diperlukan sebagai subkey adalah sebanyak Nb(Nr+1), dimana Nb adalah besarnya blok data dalam satuan word. Sedangkan Nr adalah jumlah tahapan yang harus dilalui dalam satuan word. Sebagai contoh, bilamana digunakan 128 bit

(4 word) blok data dan 128 bit (4 word) kunci maka akan dilakukan 10 kali proses. Dengan demikian dari rumus didapatkan 4(10+1)=44 word=1408 bit kunci. Untuk melakukan pengembangan jumlah kunci yang akan dipakai dari kunci utama maka dilakukan key schedule.

Ekspansi Kunci AES

Algoritma AES mengambil kunci cipher, K, dan melakukan rutin ekspansi kunci (key expansion) untuk membentuk key schedule. Ekspansi kunci menghasilkan total Nb(Nr+1) word. Algoritma ini membutuhkan set awal key yang terdiri dari Nb word, dan setiap round Nr membutuhkan data kunci sebanyak Nb word.

Hasil key schedule terdiri dari array 4 byte word linear yang dinotasikan dengan [wi]. SubWord adalah fungsi yang mengambil 4 byte word input dan mengaplikasikan S-Box ke tiap-tiap data 4 byte untuk menghasilkan word output. Fungsi RotWord mengambil word [a0, a1, a2, a3] sebagai input, melakukan permutasi siklik, dan mengembalikan word [a1, a2, a3, a0]. Rcon[i] terdiri dari nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x (x dinotasikan sebagai {02} dalam field GF(28)). Word ke Nk pertama pada ekspansi kunci berisi kunci cipher10.

Setiap word berikutnya, w[i], sama dengan XOR dari word sebelumnya, w[i-1] dan word Nk yang ada pada posisi sebelumnya, w[i-Nk]. Untuk word pada posisi yang merupakan kelipatan Nk, sebuah transformasi diaplikasikan pada w[i-1] sebelum XOR, lalu dilanjutkan oleh XOR dengan konstanta round, Rcon[i]. Transformasi ini terdiri dari pergeseran siklik dari byte data dalam suatu word RotWord, lalu diikuti aplikasi dari lookup Tabel untuk semua 4 byte data dari word SubWord.

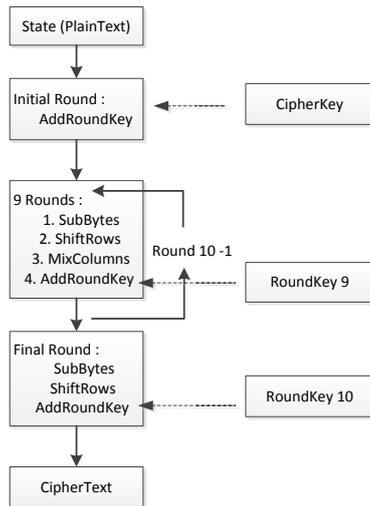
Enkripsi AES

Proses enkripsi pada algoritma Advanced Encryption Standard terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns. Diagram alur proses enkripsi pada algoritma Advanced Encryption Standard dapat dilihat pada gambar 2.

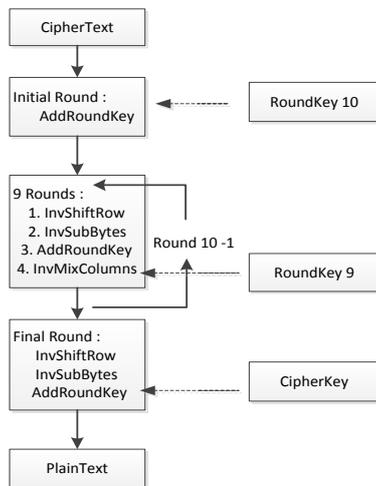
Dekripsi AES

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan

AddRoundKey. Diagram alur proses dekripsi pada algoritma *Advanced Encryption Standard* dapat dilihat pada gambar 3.



Gambar 2. Diagram Alur Proses Enkripsi AES



Gambar 3. Diagram Alur Proses Dekripsi AES

Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata steganografi berasal dari bahasa Yunani yang berarti “tulisan tersembunyi” (*covered writing*). Steganografi membutuhkan dua properti yaitu wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video [6].

Steganografi berbeda dengan kriptografi, letak perbedaannya adalah hasil keluarannya. Hasil dari kriptografi biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan dan dapat dikembalikan ke bentuk semula. Sedangkan steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi disini oleh indera manusia, tetapi

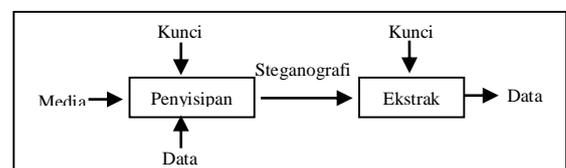
tidak oleh komputer atau perangkat pengolah digital lainnya [2].

Sejarah Steganografi

Teknik steganografi sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan *hieroglyphic* yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia [1].

Proses Steganografi

Secara umum, terdapat dua proses utama didalam steganografi. Yaitu proses penyisipan (*Embedding/encoding*) untuk menyembunyikan pesan dan ekstraksi (*extraction/decoding*) untuk mengekstraksi pesan yang disembunyikan. Pesan dapat berupa *plaintext*, *chiphertext*, citra atau apapun yang dapat ditempelkan ke dalam *bit-stream*. *Embedding* merupakan proses menyisipkan pesan ke dalam *file* yang belum dimodifikasi, yang disebut media *cover* (*cover object*). Kemudian media *cover* dan pesan yang ditempelkan membuat media *stego* (*stego object*). *Extraction* adalah proses menguraikan pesan yang tersembunyi dalam media *stego*. Suatu kunci khusus (*stego key*) juga dapat digunakan secara tersembunyi, pada saat penguraian selanjutnya dari pesan. Ringkasnya steganografi adalah teknik menanamkan *embedded message* pada suatu *cover object*, dimana hasilnya berupa *stego object*. Pihak yang terkait dengan steganografi antara lain *embeddor*, *extractor*, dan *stegoanalyst*. Skema penyisipan dan ekstraksi dalam steganografi diperlihatkan pada Gambar 4.



Gambar 4. Skema penyisipan dan ekstraksi dalam steganografi

Disk Operating System (DOS)

Disk Operating System atau disingkat dengan DOS adalah sistem operasi yang menggunakan *interface command-line* yang digunakan para pengguna komputer pada dekade tahun 1980-an. Sekarang DOS menjadi istilah generik bagi setiap sistem operasi yang dimuat dari perangkat penyimpanan berupa *disk* saat sistem komputer dinyalakan. DOS merupakan sistem yang digunakan untuk mengelola seluruh sumber daya pada sistem komputer, yaitu sumber daya *hardware* dan *software*.

DOS dapat berguna sebagai perangkat penolong ketika *Windows* tidak dapat dijalankan

dengan baik dan dapat mengakses *hard drive* tanpa GUI dan mampu melakukan proses diagnosa dan pemecahan masalah sistem.

HASIL DAN PEMBAHASAN

DESKRIPSI SISTEM

Sistem kriptografi pada pesan teks, isi *file* dokumen, dan *file* dokumen menggunakan metode algoritma *Advanced Encryption Standard* serta pendukung keamanan steganografi dalam penyembunyian pesan atau *file* dalam *file* citra merupakan penggabungan dua teknik pengamanan data yang akan diimplementasikan ke sebuah *Application Data Security System – Crypto AES And Stegano* (Fres-CAESAS) yang dirancang atau dibuat oleh penulis pada penelitian ini.

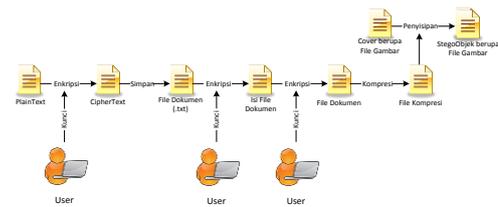
Application Data Security System - Crypto AES And Stegano (Fres-CAESAS)

Application Data Security System - Crypto AES And Stegano atau disingkat oleh penulis atau pembuat aplikasi ini yaitu dengan sebutan *Application “Fres-CAESAS”*. Fres diambil dari kependekan nama penulis atau pembuat aplikasi ini sedangkan CAESAS sendiri dari kependekan *Crypto AES And Stegano*. Aplikasi Fres-CAESAS merupakan sebuah aplikasi sistem keamanan data yang menggunakan teknik penyamaran dan penyandian yang disebut dengan teknik *Cryptography* dengan menggunakan algoritma *Advanced Encryption Standard* (AES) dan teknik penyisipan atau penyembunyian yang disebut dengan teknik *Steganography* yang salah satu penerapannya dengan penyembunyian sebuah data yang dimasukkan ke dalam sebuah gambar. Pada Aplikasi Fres-CAESAS ini terdapat 3 macam teknik keamanan data yang disediakan oleh pembuat aplikasi ini. Teknik pertama adalah teknik dengan *Cryptography*, teknik kedua adalah teknik dengan *Steganography*, dan terakhir atau ketiga adalah teknik yang telah dikombinasikan antara *Cryptography* dengan *Steganography* pada sebuah data. Adapun dalam penggunaannya, *user* bisa memilih apakah akan menggunakan teknik pertama atau kedua atau ketiga atau mengkombinasikan sendiri sesuai keinginan *user* dalam menjaga keamanan datanya.

Alur Sistem Application Fres-CAESAS

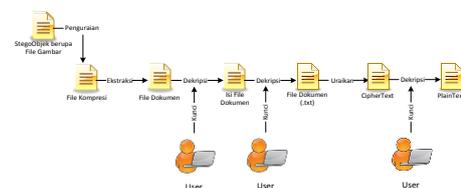
Alur sistem *Application Fres-CAESAS* pada penelitian ini adalah hasil gabungan teknik pengamanan data yang memanfaatkan kriptografi menggunakan metode *Advanced Encryption Standard* untuk melakukan enkripsi pada pesan teks (*plaintext*) dengan kunci (*key*) yang hanya diketahui oleh *user* tanpa ada pihak lain yang mengetahuinya sehingga informasi yang terkandung dalam pesan teks (*plaintext*) tidak dapat diketahui oleh pihak manapun yang tidak diinginkan, kemudian hasilnya yaitu *ciphertext* disimpan menjadi *file* dokumen berupa *file *.txt* yang selanjutnya isi (teks) daripada *file* dokumen tersebut

di enkripsi dengan kunci (*key*) oleh *user* dengan kunci (*key*) yang berbeda. Selanjutnya hasil pada *file* dokumen yang telah di enkripsi isi *file* dokumen tadi selanjutnya dienkripsi lagi *file* dokumennya dengan kunci (*key*) oleh *user* dengan kunci yang berbeda. Hasil dari *file* dokumen tersebut kemudian di kompresi menjadi *file* kompresi. Pada tahap selanjutnya memanfaatkan proses steganografi dimana pada *file* kompresi tersebut disisipkan atau disembunyikan dalam sebuah *file* gambar. Maka hasil daripada *file* gambar tersebut menjadi *file* gambar yang didalamnya terdapat sebuah *file* atau pesan rahasia. Perancangan sistem dengan melakukan enkripsi dan penyisipan pesan rahasia yang dideskripsikan sebelumnya, dapat diilustrasikan pada gambar 5.



Gambar 5. Diagram Alur Sistem – *Encryption and Hidden*

Sedangkan untuk mengembalikan (dekripsi) *file* gambar yang didalamnya terdapat sebuah *file* atau pesan rahasia dapat dilakukan dengan memanfaatkan steganografi untuk memunculkan *file* rahasia tersebut yang disimpan menjadi *file* kompresi. Hasil dari *file* kompresi tersebut selanjutnya diuraikan atau diekstraksi. Kemudian *file* ekstraksi yang di dalamnya terdapat sebuah *file* dokumen yang telah dienkripsi tersebut didekripsi dengan kunci yang sama pada kata kunci enkripsi *file* dokumen yang dibuat oleh *user*. Hasil dari dekripsi *file* dokumen tersebut, didekripsi lagi dengan kunci yang sama pada kata kunci enkripsi isi *file* dokumen yang dibuat oleh *user*. Kemudian hasil dari dekripsinya yaitu isi *file* dokumen tersebut ditampilkan pada *chiphertext* yang selanjutnya didekripsi lagi dengan kunci yang sama pada enkripsi pesan teks (*plaintext*) yang dibuat oleh *user*. Maka hasil daripada pesan teks (*plaintext*) yang dimana menjadi sebuah pesan rahasia asli tersebut, dapat dilihat pada *plainteks*. Perancangan sistem dengan melakukan dekripsi dan menampilkan pesan rahasia yang dideskripsikan sebelumnya, dapat diilustrasikan pada gambar 6.



Gambar 6. Diagram Alur Sistem - *UnHidden and Decryption*

IMPLEMENTASI SISTEM

Log In Fres-CAESAS

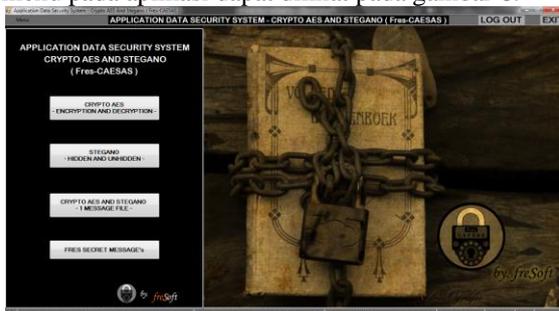
Langkah awal dalam menjalankan *Application* Fres-CAESAS yaitu buka *Application* Fres - *Crypto AES And Stegano* (Fres-CAESAS), kemudian akan muncul tampilan awal (utama) aplikasi Fres-CAESAS yaitu *Main Display* yang di dalamnya terdapat *form Log In*, dapat dilihat pada gambar 7. Pada *form Log In* tersebut, *user* harus memasukkan *username* dan *password* yang dimana nama *user* (*username*) dan kata sandi (*password*) itu telah dimiliki oleh *user*.



Gambar 7. Main Display & Log In

Menu Application Fres-CAESAS

Pada *Menu Application* Fres-CAESAS ini menampilkan *form-form menu* berupa tombol-tombol aplikasi yang terdapat dalam aplikasi guna menjalankan proses Aplikasi Fres-CAESAS tersebut. *Form-form* dalam Aplikasi Fres-CAESAS adalah *form Crypto AES – Encryption and Decryption*, *form Stegano – Hidden and UnHidden*, *form Crypto AES and Stegano – 1 Message Files*, dan terakhir *form Fres Secret Message's*. Tampilan menu pada aplikasi dapat dilihat pada gambar 8.



Gambar 8. Display Menu Application

Form Crypto AES And Stegano - 1 Message Files

One Message Files merupakan suatu proses yang khusus dibuat dengan membuat sebuah pesan rahasia (pesan teks) sendiri yang kemudian menjadi sebuah *file* dokumen (*one file document*) yang diamankan dengan beberapa proses tahapan demi menjaga keamanan pesan atau *file* rahasia tersebut.

Apabila *user* ingin masuk dan memproses dalam menjaga keamanan data dengan kombinasi atau penggabungan antara teknik kriptografi menggunakan algoritma AES dan steganografi, maka *user* akan meng-klik tombol “*Crypto AES And Stegano – 1 Message Files*” dan akan muncul *form Display of Crypto AES And Stegano – 1 Message*

Files dimana awal tampilan tersebut merupakan *Display of Encryption and Hidden – One Message Files*, dapat dilihat pada gambar 9. Pada *form Display of Crypto AES And Stegano – 1 Message Files* ini terdapat 2 sub menu dalam 1 *form* menu yaitu sub menu pertama adalah sub menu *Encryption and Hidden – One Message Files*, dan sub menu kedua adalah *Decryption and UnHidden – One Message Files*.



Gambar 9. Display of Crypto AES And Stegano – 1 Message Files (Display of Encryption and Hidden – One Message Files)

PENGUJIAN SISTEM

Pada tahap ini, akan dilakukan sebuah pengujian sistem dari *Application* Fres-CAESAS yaitu difokuskan pada enkripsi dan dekripsi kriptografi AES pada proses *Encryption and Hidden* and *Decryption and UnHidden* (*form 1 Message Files*) terhadap pesan teks (*plaintext*), isi *file* dokumen, dan *file* dokumen.

Pengujian sistem ini bertujuan untuk menguji tingkat keberhasilan perangkat lunak (*software*) *Application* Fres-CAESAS tersebut dalam mengenkripsi dengan menggunakan kunci dan mendekripsi dengan menggunakan kunci yang cocok sehingga akan mengembalikan sebuah data informasi ke bentuk semula agar dapat dibaca data informasi tersebut dan menggunakan kunci yang tidak cocok terhadap sebuah pesan teks (*plaintext*), isi *file* dokumen, dan *file* dokumen. Tampilan pesan teks (*plaintext*) dapat dilihat pada gambar 10.

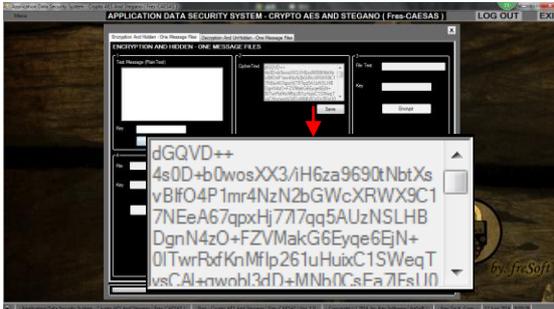


Gambar 10. Display of Original Text Message (Plaintext)

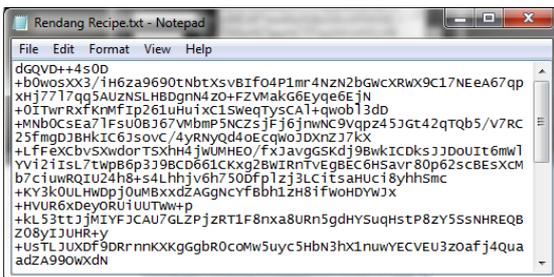
Pengujian Terhadap Pesan Teks (Plaintext) Terenkripsi

Pengujian enkripsi terhadap sebuah pesan teks (*plaintext*) dimana pesan teks (*plaintext*) yang terenkripsi tersebut masih dapat dibuka namun pesan teks (*plaintext*) menjadi teracak dan tersamarkan

(*ciphertext*) sehingga informasi tersebut tidak dapat dimengerti. Tampilan hasil pesan teks (*plaintext*) yang terenkripsi dapat dilihat pada gambar 11, dan hasil pesan teks (*plaintext*) yang terenkripsi, yang disimpan ke dalam sebuah *file* dokumen dengan *type format file extension* *.txt dapat dilihat pada gambar 12.



Gambar 11. Display of Text Message (PlainText) Encrypted Output



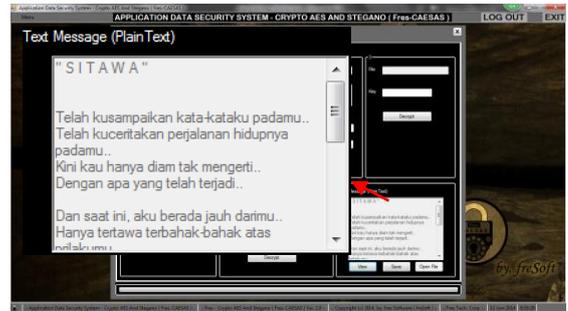
Gambar 12. Display of Text Message (PlainText) Encrypted Extension *.txt Output

Pengujian Terhadap Pesan Teks Terdekripsi

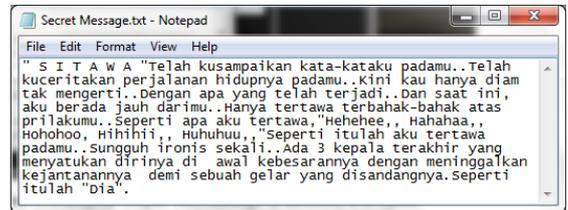
Pengujian dekripsi terhadap sebuah pesan teks (*plaintext*) dimana pesan teks (*plaintext*) yang terdekripsi dengan kunci yang cocok tersebut dapat kembali ke pesan teks aslinya sehingga informasi dapat di mengerti. Tampilan informasi dan hasil pesan teks (*plaintext*) yang terdekripsi dengan kunci yang cocok dapat dilihat pada gambar 13 dan 14, dan hasil pesan teks (*plaintext*) yang terdekripsi, yang disimpan ke dalam sebuah *file* dokumen dengan *type format file extension* *.txt dapat dilihat pada gambar 15.



Gambar 13. Display of Information Text Message (PlainText) Decrypted Output With a Key Match

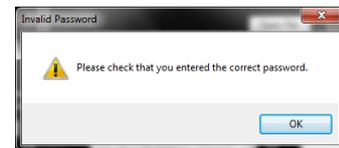


Gambar 14. Display of Text Message (PlainText) Decrypted Output With a Key Match



Gambar 15. Display of Text Message (PlainText) Decrypted Extension *.txt Output With a Key Match

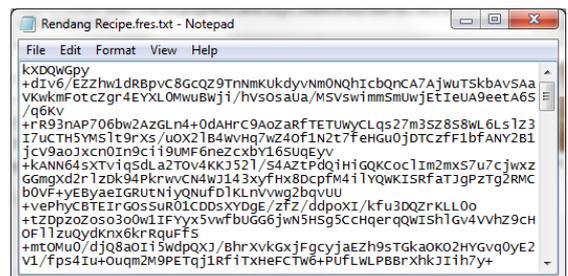
Pengujian dekripsi dengan kunci yang tidak cocok terhadap sebuah pesan teks (*plaintext*), tidak akan menghasilkan sebuah *output* dekripsi dan hanya akan menampilkan sebuah tampilan informasi *invalid password*, dapat dilihat pada gambar 16.



Gambar 16. Display of Information Invalid Password

Pengujian Terhadap Isi File Dokumen Terenkripsi

Pengujian enkripsi terhadap sebuah isi *file* dokumen dimana isi *file* dokumen yang terenkripsi tersebut *file* dokumennya masih dapat dibuka namun isi *file* dokumen menjadi teracak dan tersamarkan (*ciphertext*) sehingga informasi tersebut tidak dapat dimengerti. Tampilan hasil isi *file* dokumen yang terenkripsi dapat dilihat pada gambar 17.



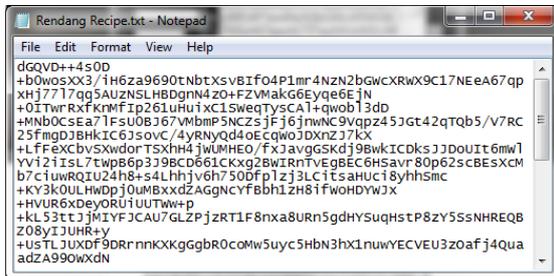
Gambar 17. Display of the Contents of the Documents Encrypted Output

Pengujian Terhadap Isi File Dokumen Terdekripsi

Pengujian dekripsi terhadap sebuah isi file dokumen dimana isi file dokumen yang terdekripsi dengan kunci yang cocok tersebut dapat kembali ke pesan teks aslinya sehingga informasi dapat di mengerti. Tampilan informasi dan hasil isi file dokumen yang terdekripsi dengan kunci yang cocok dapat dilihat pada gambar 18 dan 19.



Gambar 18. Display of Information the Contents of The Documents Decrypted Output With a Key Match

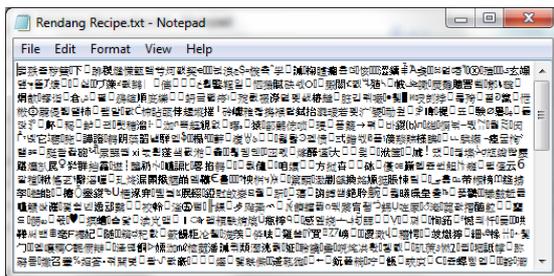


Gambar 19. Display of the Contents of The Documents Decrypted Output With a Key Match

Pengujian dekripsi dengan kunci yang tidak cocok terhadap sebuah pesan teks (plaintext), akan menampilkan sebuah tampilan informasi Error, dapat dilihat pada gambar 20 dan menghasilkan sebuah output dekripsi dimana pesan teks atau informasi tersebut tidak bisa dibaca maupun dimengerti, dapat dilihat pada gambar 21.



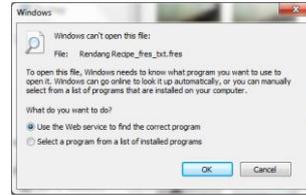
Gambar 20. Display of Information Error



Gambar 21. Display of the Contents of The Documents Decrypted Output With an UnMatch Key

Pengujian Terhadap File Dokumen Terenkripsi

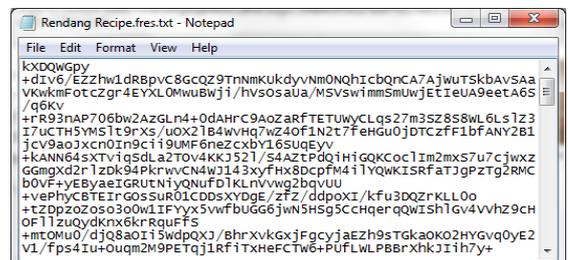
Pengujian enkripsi terhadap sebuah file dokumen dimana file dokumen yang terenkripsi tersebut file dokumennya tidak dapat dibuka. Tampilan informasi pada hasil file dokumen yang terenkripsi dapat dilihat pada gambar 22.



Gambar 22. Display of Information File Documents Decrypted Output

Pengujian Terhadap File Dokumen Terdekripsi

Pengujian dekripsi terhadap sebuah file dokumen dimana file dokumen yang terdekripsi dengan kunci yang cocok tersebut dapat kembali sehingga file dokumen tersebut dapat dibuka. Tampilan hasil file dokumen yang terdekripsi dengan kunci yang cocok dapat dilihat pada gambar 23.



Gambar 23. Display of File Documents Decrypted Output With a Key Match

Pengujian dekripsi dengan kunci yang tidak cocok terhadap sebuah file dokumen, tidak akan menghasilkan sebuah output dekripsi dan hanya akan menampilkan sebuah tampilan informasi invalid password, contoh tampilan dapat dilihat pada gambar 16.

Pengujian Terhadap File Tersembunyi

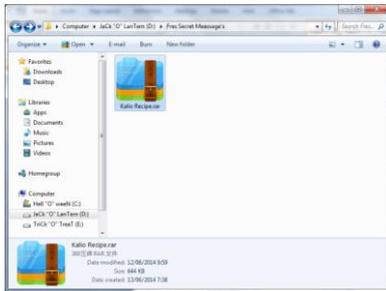
Pengujian penyembunyian file terhadap sebuah file citra (gambar) dimana file yang tersembunyi tersebut tidak dapat diketahui. Tampilan hasil file yang tersembunyi di dalam file citra (gambar) dapat dilihat pada gambar 24.



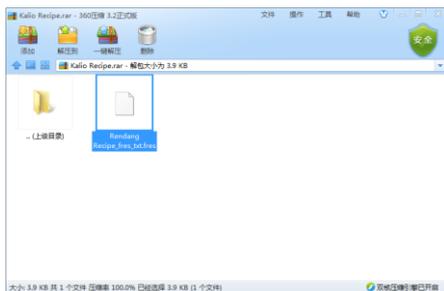
Gambar 24. Display of Hidden File Output in an Image File

Pengujian Terhadap File Terurai

Pengujian penguraian terhadap sebuah file yang tersembunyi di dalam file citra (gambar) dimana file yang terurai dapat kembali sehingga file tersebut dapat dibuka. Tampilan hasil file yang terurai dapat dilihat pada gambar 23 dan 24.



Gambar 25. Display of Extracted File Output is a File Compression



Gambar 26. Display of Secret File Output in a File Compression

PERCOBAAN DAN ANALISIS HASIL PERCOBAAN SISTEM

Pada tahap ini, akan dilakukan sebuah percobaan dan analisis hasil percobaan sistem dari aplikasi Fres-CAESAS yang dimana terdapat proses-proses encryption, decryption, hidden, and unhidden terhadap isi file dokumen, file dokumen, file kompresi, dan file citra (gambar) sebagai cover hidden.

Percobaan Sistem Terhadap Process Encrypt Output – the Contents of The Document

Tabel 2. Percobaan Sistem Terhadap Process Encrypt Output – the Contents of The Document

File Name	File Size Before Contents Encrypted	File Size After Contents Encrypted
Brownies Recipe.txt	15 bytes	44 bytes
Rendang Recipe.txt	581 bytes	1.560 bytes

Percobaan Sistem Terhadap Process Decrypt Output – the Contents of The Document

Tabel 3. Percobaan Sistem Terhadap Process Decrypt Output – the Contents of The Document

File Name	File Size Contents Encrypted	File Size After Contents Decrypted
Brownies Recipe.txt	44 bytes	15 bytes
Rendang Recipe.txt	1.560 bytes	581 bytes

Percobaan Sistem Terhadap Process Encrypt Output – File Documents

Tabel 4. Percobaan Sistem Terhadap Process Encrypt Output – File Documents

File Name	File Size Before File Encrypted	File Size After File Encrypted
Healthy Tips.docx	16.376 bytes	16.384 bytes
Safety Tips.pdf	16.926 bytes	16.928 bytes

Percobaan Sistem Terhadap Process Decrypt Output – File Documents

Tabel 5. Percobaan Sistem Terhadap Process Decrypt Output – File Documents

File Name	File Size File Encrypted	File Size After File Decrypted
Healthy Tips.docx	16.384 bytes	16.376 bytes
Safety Tips.pdf	16.928 bytes	16.926 bytes

Dari tabel percobaan sistem terhadap process encrypt dan decrypt the contents of the document dan file documents dapat disimpulkan bahwa pesan atau file rahasia setelah dilakukan proses enkripsi ukuran filenya akan lebih besar dibandingkan dengan pesan atau file rahasia aslinya atau sebelum dienkripsi. Hal itu dikarenakan adanya proses penambahan header yang berisi informasi ekstensi file. File hasil enkripsi tersebut disusun dari dua komponen yaitu komponen informasi header dan komponen data cipher. Informasi header terdiri dari 8 karakter identitas dengan karakter akhir mencatat jenis AES yang digunakan yaitu AES-128, dan ditambah dengan kunci AES yang telah diacak sebanyak 16 karakter sesuai dengan jenis AES yang digunakan yaitu AES-128. Informasi header ini sebagai pengenalan file hasil enkripsi tersebut dan digunakan untuk mendeteksi benar atau salah kunci yang digunakan pada awal proses dekripsi. Dimana pada isi file dokumen berupa plaintext yang dienkripsi menghasilkan ciphertext sehingga bytes dari file terenkripsi tersebut menjadi lebih besar.

Pada file terenkripsi setelah didekripsi file tersebut, ukuran filenya akan kembali seperti semula atau aslinya sebelum dilakukan proses enkripsi.

Percobaan Sistem Terhadap Process Hidden Output – File Compress

Tabel 6. Percobaan Sistem Terhadap Process Hidden Output – File Compress

Original Image File & Size	Secret File Name & Size	Hidden Image File & Size
	Corps of Tip.rar	
596.489 bytes	11.785 bytes	608.274 bytes
	Corps of Recipe.zip	
655.511 bytes	27.853 bytes	683.364 bytes

Percobaan Sistem Terhadap Process UnHidden Output – File Compress

Tabel 7. Percobaan Sistem Terhadap Process UnHidden Output – File Compress

Hidden Image File & Size	UnHidden Secret File Name Saved & Size
	Corps of Article.rar
608.274 bytes	608.274 bytes
	Corps of Menu.rar
655.511 bytes	683.364 bytes

Dari tabel percobaan sistem terhadap *process hidden* dan *unhidden file compress* dapat disimpulkan bahwa *file* citra (gambar) yang telah disisipkan atau disembunyikannya sebuah pesan atau *file* rahasia berupa *file* kompresi setelah dilakukan proses penyembunyian (*hidden*) *file* citra (gambar) tidak mengalami banyak perubahan yaitu citra (gambar) yang dihasilkan terlihat masih sama dengan citra (gambar) aslinya, hanya berbeda pada ukurannya yaitu ukuran *filenya* akan lebih besar dibandingkan dengan *file* citra (gambar) aslinya atau sebelum dilakukan proses *hidden*. Hal itu dikarenakan *file* gambar tersebut disisipkan atau disembunyikan sebuah pesan atau *file* rahasia, dimana pada *file* gambar yang asli dengan ukuran yang asli tersebut akan bertambah dengan ukuran pesan atau *file* rahasia tersebut. Yaitu pada hasil *size bytes* dari *file* gambar ditambahkan dengan hasil *size bytes* dari *file* rahasia tersebut, sehingga gambar yang telah disisipkan sebuah pesan tersebut lebih besar ukuran (*size*) *bytesnya* yaitu hasil total dari ukuran *file* citra (gambar) dengan *file* rahasia, dibandingkan dengan *file* gambar aslinya.

Pada tabel percobaan proses *unhidden – file compress* tersebut ukuran *file* kompresi yang telah diekstraksi tersebut ukurannya masih sama dengan ukuran *file* citra (gambar) yang disembunyikan sebuah pesan atau *file* rahasia dikarenakan pada proses *unhidden* tersebut *file* citra (gambar) diubah ke dalam bentuk *file* kompresi dan belum bisa melakukan proses *decoding* yaitu mengembalikan *file* citra (gambar) ke kondisi semula, dimana ukuran citra (gambar) kembali normal tanpa ada pesan atau *file* rahasia yang tersembunyi di dalam *cover object* tersebut. Hanya saja ditekankan bahwa hasil dari ekstraksi *unhidden*, *file* rahasia berupa *file* kompresi tersebut *filenya* masih bisa dibuka dan tidak mengalami kerusakan baik *file* yang didalam *file* kompresi maupun *file* kompresi itu sendiri dan *file* yang ada didalam *file* kompresi tersebut *filenya* masih sama dengan aslinya yaitu memiliki ukuran yang sama sebelum dikompresi, karena hal terpenting dalam melakukan penyembunyian pesan atau *file* rahasia tersebut *file* rahasia itu bisa diambil dan dibuka tanpa adanya kerusakan pada informasi tersebut atau *file* rahasia tersebut, sehingga informasi tersebut dapat dibaca.

KESIMPULAN

Kesimpulan yang didapatkan dari hasil evaluasi mengenai implementasi kriptografi pengamanan data pada pesan teks, isi file dokumen, dan file dokumen dengan menggunakan algoritma *Advanced Encryption Standard* serta pendukung keamanan steganografi dalam penyembunyian pesan teks atau *file* dalam *file* citra adalah :

1. Dalam penggunaan *Application* Fres-CAESAS, *user* bebas untuk memproses pengamanan data informasinya (pesan rahasia) dengan melakukan teknik kriptografi yang terdapat beberapa macam keamanan, atau melakukan teknik steganografi, atau melakukan teknik kombinasi kriptografi dan steganografi yang di dalamnya terdapat beberapa tahapan keamanan pada sistem Aplikasi Fres-CAESAS, atau melakukan kombinasi sesuai keinginan *user* dalam pengamanan sebuah data informasi atau pesan rahasia.
2. Berdasarkan penggunaan *Application* Fres-CAESAS, bahwa sistem keamanan tersebut dibuat dengan keamanan yang berlapis-lapis atau bertahap-tahap atau serumit mungkin agar data informasi atau pesan rahasia tersebut dapat terjaga keamanannya, sehingga akan susah untuk menjebol atau terjadinya kebocoran data informasi atau pesan rahasia tersebut.
3. Ketika *file* rahasia yang disisipkan atau disembunyikan di dalam *file* citra (gambar) tersebut dapat dideteksi, *file* rahasia tersebut masih belum bisa terbaca informasinya karena masih dienkripsi *file* dokumennya, kemudian isi *file* dokumennya, dan selanjutnya pesan teksnya (*plaintext*).
4. *File* citra (gambar) yang mengalami proses penyisipan sebuah pesan rahasia atau *file* rahasia tidak mengalami banyak perubahan.

Gambar yang dihasilkan terlihat masih sama dengan citra aslinya, hanya berbeda pada ukurannya saja.

DAFTAR PUSTAKA

- [1] Ariyus, D. 2009. *Keamanan Multimedia*. Yogyakarta : Andi.
- [2] Bender. 1996. *Techniques For Data Hiding*. IBM Systems Journal.
- [3] Daemen, J; & Rijmen, V. 2001. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197.
- [4] Hariyanto, B. 2009. *Sistem Operasi*. Bandung : Informatika.
- [5] Lusiana, V. 2011. *Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128*. Jurnal Dinamika Informatika.
- [6] Munir, R. 2006. *Kriptografi*. Bandung : Penerbit Informatika.
- [7] Stallings, W. 2006. *Cryptography and Network Security Principles and Practice*. Fifth Editon. USA : Prentice Hall.
- [8] Zunaidi, M. 2013. *Steganografi, Menyembunyikan Pesan atau File Dalam Gambar Menggunakan Command/DOS*. Jurnal Ilmiah SAINTIKOM, 11-16.
- [9] <http://nash.blog.unigha.ac.id/disk-operating-system-dos/> (diakses Mei 2014).